

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
23 June 2005 (23.06.2005)

PCT

(10) International Publication Number
WO 2005/057927 A1

(51) International Patent Classification⁷: **H04N 7/167**,
H04L 9/00, H04K 1/00

(US). YOUNG, Jonathan [US/US]; 145 State Street, Newburyport, MA 01950 (US).

(21) International Application Number:
PCT/US2004/004450

(74) Agent: **GORTYCH, Joseph, E.**; MagiQ Technologies, Inc., 171 Madison Avenue, Suite 1300, New York, NY 10016 (US).

(22) International Filing Date: 13 February 2004 (13.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/519,489 13 November 2003 (13.11.2003) US

(71) Applicant (for all designated States except US): **MAGIQ TECHNOLOGIES, INC** [US/US]; 171 Madison Ave., Suite 1300, New York, NY 10016 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

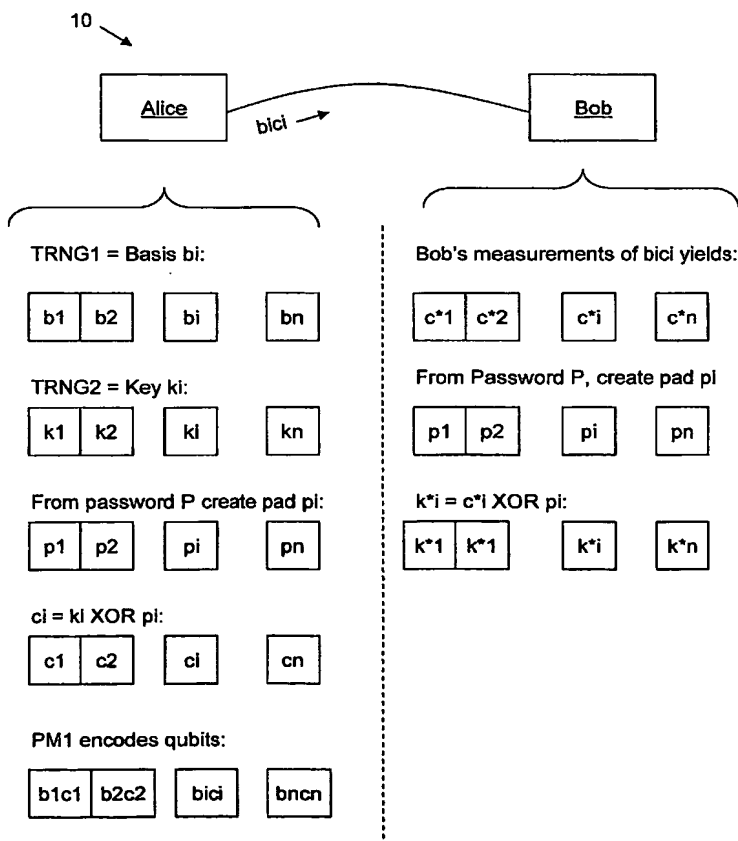
(72) Inventors; and

(75) Inventors/Applicants (for US only): **BERZANSKIS, Audrius** [LT/US]; 7 Saint Mary Road, Cambridge, MA 02139

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: QKD WITH CLASSICAL BIT ENCRYPTION



(57) Abstract: A method for enhancing the security of a quantum key distribution (QKD) system having QKD stations Alice and Bob (10) is disclosed. The method includes encrypting key bits generated by a random number generator and sent to a polarization or phase modulator to encode weak optical pulses as qubits to be shared between Alice and Bob (10). Key bit encryption is achieved by using shared password and a stream cipher. Bob obtains at least a subset of the original key bits used by Alice (10) by utilizing the same cipher stream and the shared password.



Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*